

# On the VC-Dimension of Binary Codes

Sihuang Hu  
Tel Aviv University  
sihuanghu@post.tau.ac.il

Nir Weinberger  
Tel Aviv University  
nir.wein@gmail.com

Ofer Shayevitz  
Tel Aviv University  
ofersha@eng.tau.ac.il

**Abstract**—We investigate the asymptotic rates of length- $n$  binary codes with VC-dimension at most  $dn$  and minimum distance at least  $\delta n$ . Two upper bounds are obtained, one as a simple corollary of a result by Haussler and the other via a shortening approach combining Sauer–Shelah lemma and the linear programming bound. Two lower bounds are given using Gilbert–Varshamov type arguments over constant-weight and Markov-type sets.

## I. INTRODUCTION

Let  $\mathcal{C} \subset \{0, 1\}^n$  be a binary code. In this paper, we study the relation between the size of the code and two fundamental properties: its minimum distance and its Vapnik–Chervonenkis (VC) dimension [1]. The *minimum distance* of  $\mathcal{C}$ , namely the smallest Hamming distance between any pair of codewords, plays an important role in coding theory. The *VC-dimension* of  $\mathcal{C}$  is the maximum size of a coordinate set that is *shattered* by  $\mathcal{C}$ . Recall that the projection of  $\mathcal{C}$  onto a coordinate set  $I \subseteq [n]$ , denoted  $\mathcal{C}|_I$ , is the set of all possible values assigned to these coordinates by the codewords in  $\mathcal{C}$ . We say that  $\mathcal{C}$  shatters  $I$  if  $\mathcal{C}|_I = \{0, 1\}^{|I|}$ . The VC-dimension plays an important role in statistical learning theory and computational geometry [2], [3], [4].

While this problem may be interesting in its own right, a coding-theoretic motivation is the following. Suppose a binary code  $\mathcal{C}$  with minimum distance  $\Delta$  and VC-dimension  $D$  is used over an *errors and erasures* channel. For a given number of erasures  $e$ , let  $t_e$  and  $\pi_e$  be the number of *bit errors* and the number of *error patterns*, respectively, that the code can guarantee to detect (in the remaining  $n - e$  coordinates). The error detection threshold pertaining to each of these quantities is the maximal number of erasures  $e$  such that the respective quantity is nonzero. Clearly,  $t_e > 0$  if and only if  $e < \Delta - 1$ , and  $\pi_e > 0$  if and only if  $e < n - D$ . Adopting this viewpoint, a “good code” is one that has high minimum distance and low VC-dimension. We are interested in the maximum size of such good codes.

Note that linear codes, which can be very good in the minimum distance sense as they can achieve the Gilbert–Varshamov (GV) bound [5], [6], have a VC-dimension equal to their rate, which is the highest possible (attained by any information set). More generally, binary codes drawn uniformly at random, which achieve the GV bound with high probability, also have the largest possible VC-dimension with high probability. On the other hand, the VC-dimension for a given code size is essentially minimized by a Hamming ball, which has the smallest possible minimum distance. These extremal observations demonstrate the tension between increasing the minimum distance and decreasing the VC-dimension, and also allude to the fact that in order to control both the minimum

distance and the VC-dimension, structured non-linear codes are required.

In what follows, we consider the asymptotic formulation of the problem. For any  $d, \delta \in [0, \frac{1}{2}]$ , we say that a rate  $R$  is  $(d, \delta)$ -*achievable* if there exists an infinite family of length- $n$  codes with rate at least  $R$ , VC-dimension at most  $D = dn$ , and minimum distance at least  $\Delta = \delta n$  (integer constraints are ignored as they do not affect the asymptotic behavior). We are interested in  $C(d, \delta)$ , which we define as the supremum of all  $(d, \delta)$ -achievable rates.

In Section II we derive two upper bounds for  $C(d, \delta)$ . The first is obtained as a simple asymptotic corollary of a result by Haussler [7], and the second is derived via a shortening approach that combines Sauer–Shelah lemma [8], [9] (controlling the VC-dimension) and the linear programming bound [10] (controlling the minimum distance). In Section III we present two lower bounds for  $C(d, \delta)$ . Both these bounds are obtained via GV type arguments (controlling the minimum distance) applied to constant-weight and Markov-type sets respectively (whose structure controls the VC-dimension).

## II. UPPER BOUNDS

We first briefly review upper bounds on  $C(d, \delta)$  that can be easily deduced from known results. To begin, one can clearly ignore either the minimal distance constraint or the VC-dimension constraint.

When accounting only for the minimal distance constraint, the best known upper bound is the *second MRRW bound* given by McEliece, Rodemich, Rumsey, and Welch [10] as follows:

$$R_{LP}(\delta) := \min_{0 \leq u \leq 1-2\delta} \{1 + g(u^2) - g(u^2 + 2\delta u + 2\delta)\}$$

with  $g(x) := h((1 - \sqrt{1-x})/2)$ . Here and throughout this paper we use  $h(\cdot)$  to denote the binary entropy function. The following is direct.

**Lemma 1.**  $C(d, \delta) \leq R_{LP}(\delta)$ .

When accounting only for the VC-dimension constraint, the size of a code  $\mathcal{C}$  with VC-dimension  $dn$  can be upper bounded by the Sauer–Shelah lemma [8], [9]

$$|\mathcal{C}| \leq \sum_{i=0}^{dn} \binom{n}{i} \quad (1)$$

and so the following is evident.

**Lemma 2.**  $C(d, \delta) \leq h(d)$ .

In [7] Haussler directly addressed the problem of bounding the size of codes with restricted minimal distance and VC-dimension. In his setting, the VC-dimension is a bounded

constant. However, from the results there the following bound on  $C(d, \delta)$  can still be deduced. For a number  $a \geq 0$  we define  $\langle a \rangle := \min(a, \frac{1}{2})$ . For a code  $\mathcal{C}$  we define the *unit distance graph*  $\text{UD}(\mathcal{C})$  whose vertex set is all codewords in  $\mathcal{C}$  and two codewords  $\mathbf{x}, \mathbf{y}$  are adjacent if their Hamming distance  $\text{dist}(\mathbf{x}, \mathbf{y}) = 1$ .

**Lemma 3** (Corollary to [7, Theorem 1]).

$$C(d, \delta) \leq \frac{2d}{\delta + 2d} \cdot h\left(\left\langle \frac{\delta + 2d}{2} \right\rangle\right).$$

*Proof:* Let  $\mathcal{C}$  be a length- $n$  binary code with VC-dimension at most  $dn$  and minimum distance  $\delta n$ . Suppose  $0 \leq s \leq 1$ . We randomly choose  $sn$  coordinates  $I \subseteq [n] := \{1, 2, \dots, n\}$ . For each codeword  $\mathbf{u} \in \mathcal{C}|_I$ , we define its weight  $w(\mathbf{u})$  as the number of codewords in  $\mathcal{C}$  such that its projection on  $I$  is equal to  $\mathbf{u}$ . Let  $E$  be the edge set of the unit distance graph  $\text{UD}(\mathcal{C}|_I)$ , and define the weight of an edge  $e = \{\mathbf{u}, \mathbf{v}\}$  as  $w(e) = \min\{w(\mathbf{u}), w(\mathbf{v})\}$ . Put  $W = \sum_{e \in E} w(e)$ , and note that  $W$  is a random variable depending on the random choice of  $I$ . The bound follows by estimating  $\mathbb{E}[W]$ , the expectation of  $W$ , in two ways. First, we claim that for any  $I \subset [n]$ ,

$$W \leq 2dn|\mathcal{C}|. \quad (2)$$

On the other hand, we can bound  $\mathbb{E}[W]$  from below:

$$\mathbb{E}[W] \geq \frac{sn \cdot \delta n}{n - sn + 1} \left( |\mathcal{C}| - \sum_{i=0}^{dn} \binom{sn}{i} \right). \quad (3)$$

(Please refer to [11, Lemma 5.14] for the proof of (2) and (3).) Thus we have

$$\left( ((\delta + 2d)s - 2d) - \frac{2d}{n} \right) |\mathcal{C}| \leq s\delta \sum_{i=0}^{dn} \binom{sn}{i}.$$

For any  $s > \frac{2d}{\delta + 2d}$  and sufficient large  $n$ , we can get  $|\mathcal{C}| = O(\sum_{i=0}^{dn} \binom{sn}{i})$ , and hence  $C(d, \delta) \leq s \cdot h(\langle d/s \rangle)$ . The result follows directly. ■

We shall next combine Lemma 1 and Lemma 2 to obtain an improved upper bound.

**Theorem 1.**

$$C(d, \delta) \leq \min_{0 \leq s \leq 1-2\delta} \left\{ s \cdot h\left(\left\langle \frac{d}{s} \right\rangle\right) + (1-s)R_{LP}\left(\frac{\delta}{1-s}\right) \right\}.$$

*Proof:* Let  $\mathcal{C}$  be a length- $n$  binary code with VC-dimension at most  $dn$  and minimum distance  $\delta n$ . Choose  $s \in [0, 1 - 2\delta]$ , and consider the projection of  $\mathcal{C}$  on  $[sn] = \{1, 2, \dots, sn\}$ . Of course the VC-dimension of  $\mathcal{C}|_{[sn]}$  is also at most  $dn$ , and so its rate can be bounded by Lemma 2. For any given prefix  $\mathbf{u} \in \mathcal{C}|_{[sn]}$ , we denote the set of its possible suffixes by  $\mathcal{Z}(\mathbf{u}) \subset \{0, 1\}^{(1-s)n}$ , i.e., for any  $\mathbf{v} \in \mathcal{Z}(\mathbf{u})$  there exists a codeword  $\mathbf{x} \in \mathcal{C}$  such that  $\mathbf{x}$  is the concatenation of  $\mathbf{u}$  and  $\mathbf{v}$ . Clearly,  $\mathcal{Z}(\mathbf{u})$  is a code of length  $(1-s)n$  and minimal distance  $\delta n$ , and so its rate can be bounded by the second MRRW bound. Then our result follows from

$$|\mathcal{C}| \leq |\mathcal{C}|_{[sn]} \cdot \sum_{\mathbf{u} \in \mathcal{C}|_{[sn]}} |\mathcal{Z}(\mathbf{u})|. \quad \blacksquare$$

### III. LOWER BOUNDS

A general procedure to obtain lower bounds on  $C(d, \delta)$  is the following.

- (i) Pick some subset  $S$  of the Hamming cube  $\{0, 1\}^n$  that has some “nice” structure.
- (ii) Compute a generalized GV bound for subset  $S$ , namely a lower bound on the size of the largest code of minimum distance at least  $\delta n$  where all codewords belong to  $S$ .
- (iii) Find an upper bound for the VC-dimension  $dn$  of any subset of  $S$  that has minimum distance at least  $\delta n$ .
- (iv) Combine the bounds (ii)-(iii).

In the following two subsections, we will show two ways to choose “nice” subsets of the Hamming cube and calculate the corresponding bounds.

#### A. Constant Weight Codes

Here we choose subset  $S$  to be the collection of all codewords with some constant weight.

**Lemma 4.** Suppose  $\delta \in [0, \frac{1}{2}]$  and  $w \in [0, 1]$ . Let  $\mathcal{C}$  be a binary code of length  $n$ , constant weight  $wn$ , and minimum distance  $\delta n$ . Then the VC-dimension of  $\mathcal{C}$  is at most  $(w - \delta/2)n + 1$ .

*Proof:* Suppose the VC-dimension of  $\mathcal{C}$  is  $dn$ . Without loss of generality, we assume that the first  $dn$  coordinates are shattered. Then there exist two codewords  $\mathbf{x} = x_1x_2 \dots x_n$  and  $\mathbf{y} = y_1y_2 \dots y_n$  such that  $x_i = 1$  for  $1 \leq i \leq dn$  and  $y_i = 1$  for  $1 \leq i \leq dn - 1$  and  $y_{dn} = 0$ . Hence  $|\text{supp}(\mathbf{x}) \cap \text{supp}(\mathbf{y})| \geq dn - 1$ . On the other hand,  $\text{dist}(\mathbf{x}, \mathbf{y}) = 2wn - 2|\text{supp}(\mathbf{x}) \cap \text{supp}(\mathbf{y})|$ , which is at least  $\delta n$ . Therefore  $\delta n \leq 2wn - 2|\text{supp}(\mathbf{x}) \cap \text{supp}(\mathbf{y})| \leq 2wn - 2(dn - 1)$ . This proves the result. ■

Let  $A(n, \delta n, wn)$  denote the maximum size of length- $n$  binary code with constant weight  $wn$  and minimum distance  $\delta n$ . The following GV type bound is well-known.

**Lemma 5.**

$$A(n, \delta n, wn) \geq \frac{\binom{n}{wn}}{\sum_{i=0}^{\delta n/2-1} \binom{wn}{i} \binom{n-wn}{i}}. \quad (4)$$

Now we are ready to state our first lower bound for  $C(d, \delta)$ .

**Theorem 2.** Let  $d, \delta \in [0, \frac{1}{2}]$ , and let  $w = d + \frac{\delta}{2}$ . Then

$$C(d, \delta) \geq \begin{cases} h(w) - \max_{0 \leq x \leq \delta/2} \left[ w h\left(\frac{x}{w}\right) + (1-w) h\left(\frac{x}{1-w}\right) \right] & \text{if } w < \frac{1}{2} \\ 1 - h(\delta) & \text{otherwise.} \end{cases}$$

*Proof:* If  $w < \frac{1}{2}$ , plug it into (4) and take the asymptotic form, then the result follows directly from Lemma 4. If  $w \geq \frac{1}{2}$  then set  $w = \frac{1}{2}$  in (4). ■

#### B. Markov Type

For a binary codeword  $\mathbf{x} = x_1x_2 \dots x_n \in \{0, 1\}^n$ , the number of *switches* of  $\mathbf{x}$  is equal to  $|\{i : 1 \leq i \leq n - 1, x_i \oplus x_{i+1} = 1\}|$ , in which  $\oplus$  is the XOR operation. Here we present another lower bound for  $C(d, \delta)$  based on the following observation.

**Fact 1.** Let  $S$  be the collection of all codewords in the Hamming cube  $\{0, 1\}^n$  that has at most  $dn$  switches. Then the VC-dimension of  $S$  or any subset of  $S$  is at most  $dn + 1$ .

We refer to an  $(S, M, \delta n)$ -code as a subset of  $S$  with size  $M$  and minimum distance at least  $\delta n$ . We will prove a GV type bound for such  $(S, M, \delta n)$ -codes, and thus get a lower bound for  $C(d, \delta)$ . Our proof relies on a generalized GV bound provided by Kolesnik and Krachkovsky [12], and follows the same line of reasoning as in Sections III-V of [13], where Marcus and Roth developed an improved GV bound for constrained systems based on stationary Markov chains.

**Lemma 6.** [12, Lemma 1] Let  $S$  be a subset of  $\{0, 1\}^n$ . Then there exists an  $(S, M, \delta n)$ -code such that

$$M \geq \frac{|S|^2}{4|\mathcal{B}_S(\delta n - 1)|}$$

where

$$\mathcal{B}_S(\delta n - 1) = \{(w, w') \in S \times S : \text{dist}(w, w') \leq \delta n - 1\}.$$

In order to compute our lower bound, we shall consider stationary Markov chains on graphs. A *labeled graph*  $G = (V_G, E_G, L_G)$  is a finite directed graph with vertices  $V_G$ , edges  $E_G$ , and a labeling  $L_G : E_G \rightarrow \Sigma$  for some finite alphabet  $\Sigma$ . For any vertex  $u$ , the set of outgoing edges from  $u$  is denoted by  $E_G^+(u)$ , and the set of incoming edges to  $u$  is  $E_G^-(u)$ . A graph  $G$  is called *irreducible* if there is a path in each direction between each pair of vertices of the graph. The greatest common divisor of the lengths of cycles of a graph  $G$  is called the *period* of  $G$ . An irreducible graph  $G$  with period 1 is called *primitive*. A *stationary Markov chain* on a finite directed graph  $G$  is a function  $P : E_G \rightarrow [0, 1]$  such that

- (i)  $\sum_{e \in E_G} P(e) = 1$ ;
- (ii)  $\sum_{e \in E_G^+(u)} P(e) = \sum_{e \in E_G^-(u)} P(e)$  for every  $u \in V_G$ .

We denote by  $\mathcal{M}(G)$  the set of all stationary Markov chains on  $G$ . For a stationary Markov chain  $P \in \mathcal{M}(G)$ , we introduce two dummy random variables  $X, Y$  such that their joint distribution is defined by

$$\Pr\{X = u, Y = v\} = \begin{cases} P((u, v)) & \text{if } (u, v) \in E_G \\ 0 & \text{otherwise.} \end{cases}$$

Then the condition (ii) amounts to saying that the marginal distributions of  $X$  and  $Y$  are equal.

For a stationary Markov chain  $P \in \mathcal{M}(G)$  and a function  $f : E_G \rightarrow \mathbb{R}^k$ , we denote by  $\mathbf{E}_P(f)$  the expected value of  $f$  with respect to  $P$ , that is,

$$\mathbf{E}_P(f) := \sum_{e \in E_G} P(e) f(e).$$

Fix a vertex  $u$ , and let  $\Gamma_n(G)$  denote the set of all cycles in  $G$  of length  $n$  that start and end at  $u$ . For a cycle  $\gamma = e_1 e_2 \dots e_n \in \Gamma_n(G)$ , let  $P_\gamma$  denote the stationary Markov chain defined by

$$P_\gamma(e) := \frac{1}{n} |\{i \in \{1, 2, \dots, n\} : e_i = e\}|.$$

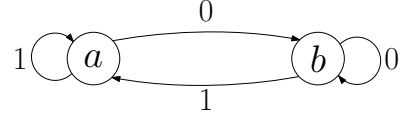


Fig. 1. labeled graph  $G$  over  $\Sigma = \{0, 1\}$

We refer to  $P_\gamma$  as the *empirical distribution* of the cycle  $\gamma$ , and to

$$\mathbf{E}_{P_\gamma}(f) = \sum_{e \in E_G} P_\gamma(e) f(e)$$

as the *empirical average* of  $f$  on the cycle  $\gamma$ . (Note that the empirical distribution  $P_\gamma$  is closely related to the so-called “second-order type” of sequence  $L_G(e_1)L_G(e_2) \dots L_G(e_n)$ .) For a subset  $U \subset \mathbb{R}^k$ , let  $\mathcal{M}(G; f, U)$  denote the set of all stationary Markov chains  $P$  on  $G$  such that  $\mathbf{E}_P(f) \in U$ , and let

$$\Gamma_n(G; f, U) := \{\gamma \in \Gamma_n(G) : \mathbf{E}_{P_\gamma}(f) \in U\}.$$

The following lemma is a consequence of well-known results on second-order types of Markov chains, cf. Boza [14], Davisson, Longo, Sgarro [15], Natarajan [16], Csiszár, Cover, Choi [17], and Csiszár [18]. (Throughout this paper, the base of the logarithm is  $|\Sigma|$ .)

**Lemma 7.** [13, Lemma 2] Let  $G$  be a primitive graph and  $f : E_G \rightarrow \mathbb{R}^k$  be a function on the edges of  $G$ . Let  $U$  be an open subset of  $\mathbb{R}^k$ . Then

$$\lim_{n \rightarrow \infty} \frac{1}{n} \log |\Gamma_n(G; f, U)| = \sup_{P \in \mathcal{M}(G; f, U)} H_P(Y|X).$$

Hereafter we will consider the labeled graph  $G$  over alphabet  $\Sigma = \{0, 1\}$  depicted in Figure 1. The labeling  $L_G$  is defined by  $L_G((a, b)) = L_G((b, b)) = 0$  and  $L_G((b, a)) = L_G((a, a)) = 1$ . On the other hand, the function  $f : E_G \rightarrow \mathbb{R}$  is defined by  $f((a, a)) = f((b, b)) = 0$  and  $f((a, b)) = f((b, a)) = 1$ . Then we can verify the following.

**Fact 2.** For a cycle  $\gamma = e_1 e_2 \dots e_n \in \Gamma_n(G)$ , the value  $n\mathbf{E}_{P_\gamma}(f) - f(e_1)$  is equal to the number of switches of the corresponding binary sequence  $L_G(e_1)L_G(e_2) \dots L_G(e_n)$ .

Now we come to our second lower bound for  $C(d, \delta)$ . We will consider the subset

$$S_n(d) = S_n([0, d]) := \{L_G(e_1)L_G(e_2) \dots L_G(e_n) : e_1 e_2 \dots e_n \in \Gamma_n(G; f, [0, d])\}.$$

By definition, for any  $x \in S_n(d)$  its number of switches is at most  $dn$ .

In order to use Lemma 6, we introduce the graph  $G \times G$  whose vertex set is  $V_{G \times G} = V_G \times V_G = \{(u, u') : u, u' \in V_G\}$  and edge set is  $E_{G \times G} = E_G \times E_G = \{(e, e') : e, e' \in E_G\}$ . Given the function  $f$  defined on the edges of  $G$ , we define two functions  $f^{(1)}$  and  $f^{(2)}$  on  $E_{G \times G}$  by

$$f^{(1)}(\langle e, e' \rangle) = f(e), \quad f^{(2)}(\langle e, e' \rangle) = f(e')$$

and a function  $\Delta : E_{G \times G} \rightarrow \mathbb{R}$  by

$$\Delta(\langle e, e' \rangle) = \begin{cases} 1 & \text{if } L_G(e) \neq L_G(e') \\ 0 & \text{otherwise.} \end{cases}$$

We collect  $f^{(1)}, f^{(2)}$  and  $\Delta$  to define a function  $\varphi : E_{G \times G} \rightarrow \mathbb{R}^3$  by  $\varphi = [f^{(1)}, f^{(2)}, \Delta]$ . For a subset  $U \subset [0, 1]$  we set

$$\mathcal{F}(U) := \sup_{P \in \mathcal{M}(G; f, U)} H_P(Y|X),$$

$$\mathcal{G}(U, \delta) := \sup_{Q \in \mathcal{M}(G \times G; \varphi, U \times U \times [0, \delta])} H_Q(Y|X).$$

In particular, we use  $\mathcal{F}(p)$  and  $\mathcal{G}(p, \delta)$  as short-hand notations for  $\mathcal{F}(\{p\})$  and  $\mathcal{G}(\{p\}, \delta)$  respectively, where  $0 \leq p \leq 1$ . Set

$$R_{MA}(d, \delta) := \sup_{p \in [0, d]} \{2\mathcal{F}(p) - \mathcal{G}(p, \delta)\}$$

$$= \sup_{p \in [0, d]} \left\{ 2 \sup_{\substack{P \in \mathcal{M}(G): \\ \mathbf{E}_P(f) = p}} H_P(Y|X) - \sup_{\substack{Q \in \mathcal{M}(G \times G): \\ \mathbf{E}_Q(f^{(i)}) = p, i=1,2 \\ \mathbf{E}_Q(\Delta) \in [0, \delta]}} H_Q(Y|X) \right\}.$$

**Lemma 8.** *There exist  $(S_n(d), M, \delta n)$ -codes satisfying*

$$\frac{\log M}{n} \geq R_{MA}(d, \delta) - o(1).$$

*Proof:* For  $p \in [0, d]$  and  $\varepsilon > 0$ , let  $U_{p, \varepsilon} = (p - \varepsilon, p + \varepsilon)$ ,

$$S_n(U_{p, \varepsilon}) := \{L_G(e_1)L_G(e_2) \cdots L_G(e_n) : e_1 e_2 \cdots e_n \in \Gamma_n(G; f, U_{p, \varepsilon})\},$$

and

$$\mathcal{B}_{S_n(U_{p, \varepsilon})}(\delta n - 1) := \{(\mathbf{w}, \mathbf{w}') \in S_n(U_{p, \varepsilon}) \times S_n(U_{p, \varepsilon}) : \text{dist}(\mathbf{w}, \mathbf{w}') \leq \delta n - 1\}.$$

By Lemma 7,

$$\lim_{n \rightarrow \infty} \frac{1}{n} \log |S_n(U_{p, \varepsilon})| = \lim_{n \rightarrow \infty} \frac{1}{n} \log |\Gamma_n(G; f, U_{p, \varepsilon})|$$

$$= \mathcal{F}(U_{p, \varepsilon}),$$

$$\lim_{n \rightarrow \infty} \frac{1}{n} \log |\mathcal{B}_{S_n(U_{p, \varepsilon})}(\delta n - 1)|$$

$$= \lim_{n \rightarrow \infty} \frac{1}{n} \log |\Gamma_n(G \times G; \varphi; U_{p, \varepsilon} \times U_{p, \varepsilon} \times [0, \delta])|$$

$$= \mathcal{G}(U_{p, \varepsilon}, \delta).$$

Note that both  $H_P(Y|X)$  and  $\mathbf{E}_P(f)$  are continuous in  $P$ . So letting  $\varepsilon \rightarrow 0$ , then by Lemma 6 there exist  $(S_n(d), M, \delta n)$ -codes satisfying

$$\frac{\log M}{n} \geq 2\mathcal{F}(p) - \mathcal{G}(p, \delta) - o(1).$$

Then our result follows.  $\blacksquare$

**Theorem 3.**  $C(d, \delta) \geq R_{MA}(d, \delta)$ .

*Proof:* This follows from Lemma 8 and the fact that any  $(S_n(d), M, \delta n)$  code has VC-dimension at most  $dn + 1$ .  $\blacksquare$

Using convex duality we can compute  $R_{MA}(d, \delta)$  through an unconstrained optimization problem with convex objective function as follows. For a function  $f : E_G \rightarrow \mathbb{R}^k$ , let  $A_{G;f}(\mathbf{x})$ ,  $\mathbf{x} \in \mathbb{R}^k$ , be the matrix function indexed by the states of  $G$  with entries

$$[A_{G;f}(\mathbf{x})]_{u,v} = \begin{cases} 2^{-\mathbf{x} \cdot f((u,v))} & \text{if } (u, v) \in E_G \\ 0 & \text{otherwise.} \end{cases}$$

and let  $\lambda_{G;f}(\mathbf{x})$  denote the spectral radius of  $A_{G;f}(\mathbf{x})$ . Recall the definitions of  $f, f^{(1)}, f^{(2)}$  and  $\Delta$ , and define  $\varphi' = [f^{(1)} + f^{(2)}, \Delta] : E_{G \times G} \rightarrow \mathbb{R}^2$ . Let  $G$  be the graph of Figure 1. Then

$$A_{G;f}(\mathbf{x}) = \begin{matrix} & \begin{matrix} a & b \end{matrix} \\ \begin{matrix} a \\ b \end{matrix} & \begin{bmatrix} 1 & 2^{-x} \\ 2^{-x} & 1 \end{bmatrix} \end{matrix}$$

and

$$A_{G \times G; \varphi'}(\mathbf{x}, \mathbf{z}) = \begin{matrix} & \begin{matrix} \langle a, a \rangle & \langle a, b \rangle & \langle b, a \rangle & \langle b, b \rangle \end{matrix} \\ \begin{matrix} \langle a, a \rangle \\ \langle a, b \rangle \\ \langle b, a \rangle \\ \langle b, b \rangle \end{matrix} & \begin{bmatrix} 1 & 2^{-x-z} & 2^{-x-z} & 2^{-2x} \\ 2^{-x} & 2^{-z} & 2^{-2x-z} & 2^{-x} \\ 2^{-x} & 2^{-2x-z} & 2^{-z} & 2^{-x} \\ 2^{-2x} & 2^{-x-z} & 2^{-x-z} & 1 \end{bmatrix} \end{matrix}.$$

Through direct computations, we have  $\lambda_{G;f}(\mathbf{x}) = 2^{-x} + 1$ , and

$$\lambda_{G \times G; \varphi'}(\mathbf{x}, \mathbf{z}) = \frac{1}{2} \left( (4^{-x} + 1)(2^{-z} + 1) + \sqrt{(4^{-x} + 1)^2 4^{-z} - 2(16^{-x} - 6 \cdot 4^{-x} + 1)2^{-z} + (4^{-x} + 1)^2} \right).$$

From the well-known results in convex duality principle, we can obtain the following. Similar results are also obtained in [19], [20].

**Lemma 9.** [13, Lemma 5] *Let  $G$  be a graph and let  $f : E_G \rightarrow \mathbb{R}^k, g : E_G \rightarrow \mathbb{R}^l$  be functions on the edges of  $G$ . Set  $\phi = [f, g] : E_G \rightarrow \mathbb{R}^{k+l}$ . Then for any  $\mathbf{r} \in \mathbb{R}^k$  and  $\mathbf{s} \in \mathbb{R}^l$ ,*

$$\sup_{\substack{P \in \mathcal{M}(G): \\ \mathbf{E}_P(f) = \mathbf{r} \\ \mathbf{E}_P(g) \leq \mathbf{s}}} H_P(Y|X) = \inf_{\substack{\mathbf{x} \in \mathbb{R}^k \\ \mathbf{z} \in \mathbb{R}_{\geq 0}^l}} \{\mathbf{x} \cdot \mathbf{r} + \mathbf{z} \cdot \mathbf{s} + \log \lambda_{G; \phi}(\mathbf{x}, \mathbf{z})\}.$$

**Theorem 4.**

$$R_{MA}(d, \delta)$$

$$= \sup_{p \in [0, d]} \left\{ 2h(p) - \inf_{\substack{\mathbf{x} \in \mathbb{R}^k \\ \mathbf{z} \in \mathbb{R}_{\geq 0}^l}} \{2p\mathbf{x} + \delta\mathbf{z} + \log \lambda_{G \times G; \varphi'}(\mathbf{x}, \mathbf{z})\} \right\}.$$

*Proof:* Applying Lemma 9 to compute  $\mathcal{F}(p)$ , we have

$$\mathcal{F}(p) = \inf_{\mathbf{x} \in \mathbb{R}} \{p\mathbf{x} + \log \lambda_{G;f}(\mathbf{x})\}$$

$$= \inf_{\mathbf{x} \in \mathbb{R}} \{p\mathbf{x} + \log(2^{-x} + 1)\}$$

$$= h(p).$$

Note that the function  $\log \lambda_{G; \phi}(\mathbf{x}, \mathbf{z})$  in Lemma 9 is convex (see [13, Remark 2]). Thus a similar argument can show that

$$\mathcal{G}(p, \delta) = \inf_{\substack{\mathbf{x} \in \mathbb{R} \\ \mathbf{z} \in \mathbb{R}_{\geq 0}^l}} \{2p\mathbf{x} + \delta\mathbf{z} + \log \lambda_{G \times G; \varphi'}(\mathbf{x}, \mathbf{z})\}.$$

$\blacksquare$

#### IV. EXAMPLES

**Example 1.** We plot the bounds for  $d = \frac{1}{4}$  and  $\frac{1}{16}$  in Fig. 2. Note that all these bounds intersect at  $R = h(d)$  when  $\delta = 0$ ; and our shortening upper bound (Thm. 1) is always better than the second MRRW bound (hence we do not plot it here). As we can see, for  $d = \frac{1}{4}$  our shortening upper bound (Thm. 1) is always better than Haussler's upper bound (Lem. 3), and the constant weight lower bound (Thm. 2) is always better



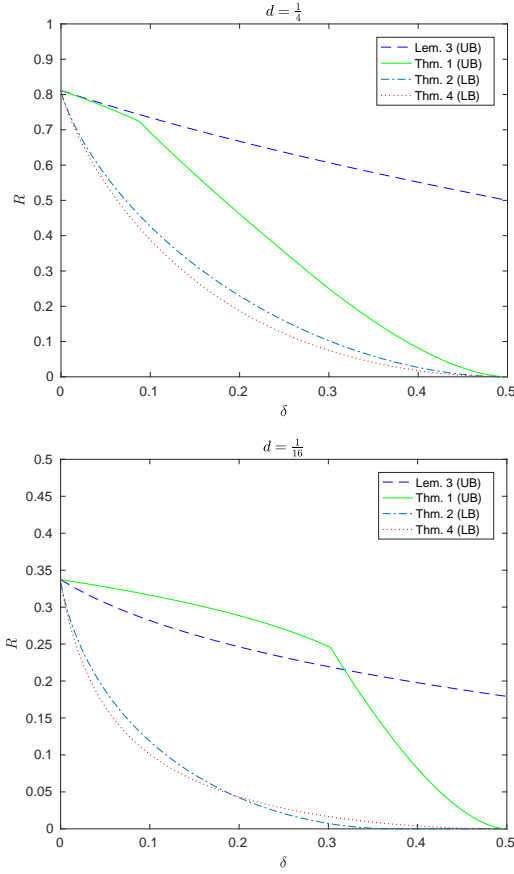


Fig. 2. Bounds for  $d = \frac{1}{4}$  and  $d = \frac{1}{16}$

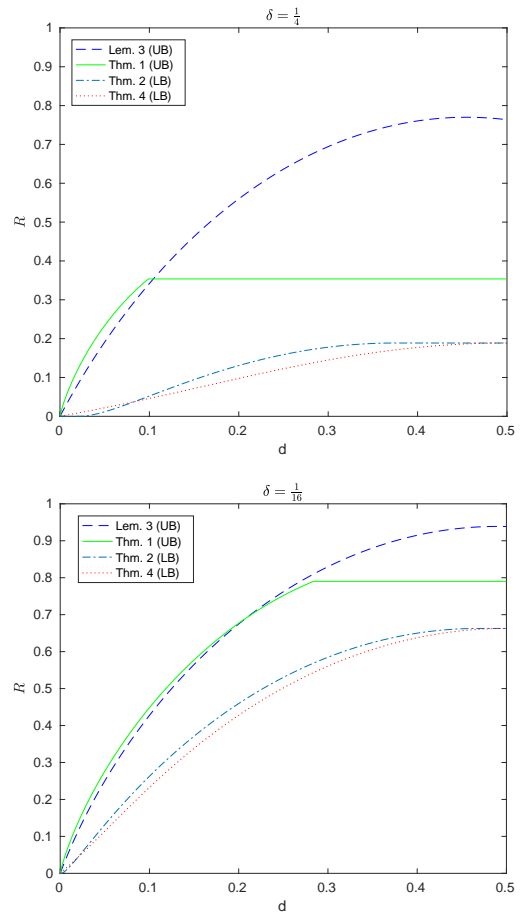


Fig. 3. Bounds for  $\delta = \frac{1}{4}$  and  $\delta = \frac{1}{16}$

than the Markov type lower bound (Thm. 3). For  $d = \frac{1}{16}$ , the performance of these bounds are quite different.

**Example 2.** We plot the bounds for  $\delta = \frac{1}{4}$  and  $\frac{1}{16}$  in Fig. 3.

## REFERENCES

- [1] V. N. Vapnik and A. J. Červonenkis, "The uniform convergence of frequencies of the appearance of events to their probabilities," *Teor. Veroyatnost. i Primenen.*, vol. 16, pp. 264–279, 1971.
- [2] R. M. Dudley, "Central limit theorems for empirical measures," *Ann. Probab.*, vol. 6, no. 6, pp. 899–929, 1978.
- [3] D. Haussler and E. Welzl, "ε-nets and simplex range queries," *Discrete Comput. Geom.*, vol. 2, no. 2, pp. 127–151, 1987.
- [4] A. Blumer, A. Ehrenfeucht, D. Haussler, and M. K. Warmuth, "Learnability and the Vapnik-Chervonenkis dimension," *J. Assoc. Comput. Mach.*, vol. 36, no. 4, pp. 929–965, 1989.
- [5] E. Gilbert, "A comparison of signalling alphabets," *Bell System Technical Journal*, vol. 31, no. 3, pp. 504–522, May 1952.
- [6] R. R. Varšamov, "The evaluation of signals in codes with correction of errors," *Dokl. Akad. Nauk SSSR (N.S.)*, vol. 117, pp. 739–741, 1957.
- [7] D. Haussler, "Sphere packing numbers for subsets of the boolean n-cube with bounded Vapnik-Chervonenkis dimension," *Journal of Combinatorial Theory, Series A*, vol. 69, no. 2, pp. 217–232, 1995.
- [8] N. Sauer, "On the density of families of sets," *J. Combinatorial Theory Ser. A*, vol. 13, pp. 145–147, 1972.
- [9] S. Shelah, "A combinatorial problem; stability and order for models and theories in infinitary languages," *Pacific J. Math.*, vol. 41, pp. 247–261, 1972.
- [10] R. J. McEliece, E. R. Rodemich, H. Rumsey, Jr., and L. R. Welch, "New upper bounds on the rate of a code via the Delsarte-MacWilliams inequalities," *IEEE Trans. Information Theory*, vol. 23, no. 2, pp. 157–166, 1977.
- [11] J. Matouek, *Geometric discrepancy*, ser. Algorithms and Combinatorics. Springer-Verlag, Berlin, 2010, vol. 18, an illustrated guide, Revised paperback reprint of the 1999 original.
- [12] V. D. Kolesnik and V. Y. Krachkovsky, "Generating functions and lower bounds on rates for limited error-correcting codes," *IEEE Trans. Inform. Theory*, vol. 37, no. 3, part 2, pp. 778–788, 1991.
- [13] B. H. Marcus and R. M. Roth, "Improved Gilbert-Varshamov bound for constrained systems," *IEEE Trans. Inform. Theory*, vol. 38, no. 4, pp. 1213–1221, 1992.
- [14] L. B. Boza, "Asymptotically optimal tests for finite Markov chains," *Ann. Math. Statist.*, vol. 42, pp. 1992–2007, 1971.
- [15] L. D. Davisson, G. Longo, and A. Sgarro, "The error exponent for the noiseless encoding of finite ergodic Markov sources," *IEEE Trans. Inform. Theory*, vol. 27, no. 4, pp. 431–438, 1981.
- [16] S. Natarajan, "Large deviations, hypotheses testing, and source coding for finite Markov chains," *IEEE Trans. Inform. Theory*, vol. 31, no. 3, pp. 360–365, 1985.
- [17] I. Csiszár, T. M. Cover, and B. S. Choi, "Conditional limit theorems under Markov conditioning," *IEEE Trans. Inform. Theory*, vol. 33, no. 6, pp. 788–801, 1987.
- [18] I. Csiszár, "The method of types," *IEEE Trans. Inform. Theory*, vol. 44, no. 6, pp. 2505–2523, 1998, information theory: 1948–1998.
- [19] J. Justesen and T. Høholdt, "Maxentropic Markov chains," *IEEE Trans. Inform. Theory*, vol. 30, no. 4, pp. 665–667, 1984.
- [20] B. Marcus and S. Tuncel, "Entropy at a weight-per-symbol and embeddings of Markov chains," *Invent. Math.*, vol. 102, no. 2, pp. 235–266, 1990.